



45

PATENT  
450110-03707

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants : Jonathan James STONE et al.  
Serial No. : 10/006,481  
Filed : December 6, 2001  
For : WATERMARKING AND TRANSFERRING MATERIAL  
Art Unit : 2121

745 Fifth Avenue  
New York, New York 10151  
Tel. (212) 588-0800

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:  
Assistant Commissioner for Patents  
Washington, D.C. 20231, on February 13, 2002

Glenn F. Savit, Reg. No. 37,437

Name of Applicant, Assignee or  
Registered Representative

Signature

February 13, 2002

Date of Signature

CLAIM OF PRIORITY

Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

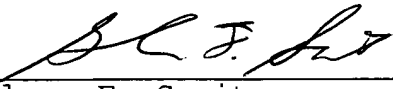
In support of the claim of priority under 35. U.S.C. § 119 asserted in the Declaration accompanying the above-entitled application, as filed, please find enclosed herewith certified copies of U.K. Application Nos. 0029851.3 and 0121202.6, filed in U.K. on 7 December 2000 and 31 August 2001, respectively, forming the basis for such claim.

PATENT  
450110-03707

Acknowledgment of the claim of priority and of the  
receipt of said certified copy(s) is requested.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP  
Attorneys for Applicants

By:   
Glenn F. Savit  
Reg. No. 37,437  
Tel. (212) 588-0800

Enclosure(s)



INVESTOR IN PEOPLE

The Patent Office  
Concept House  
Cardiff Road  
Newport  
South Wales  
NP10 8QQ

## CERTIFIED COPY OF PRIORITY DOCUMENT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

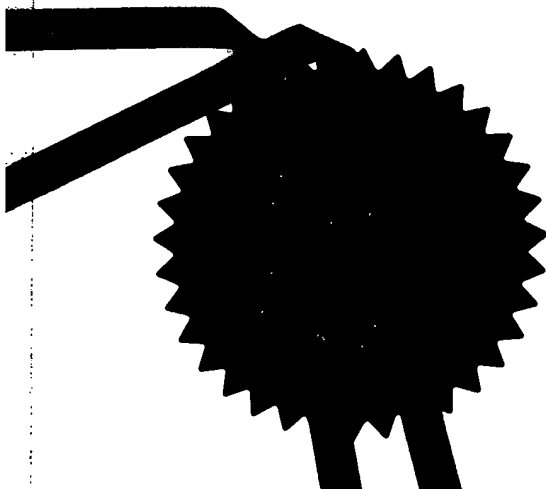
In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

*W. Evans*

Dated 28 November 2001





## Request for a grant of a patent

(See the notes on the back of this form you can also get an explanatory leaflet from the Patent Office to help you fill in this form)

Cardiff Road  
Newport  
Gwent NP9 1RH

1. Your reference P010406GB RWP

2. Patent application number  
(The Patent Office will fill in this part)

07 DEC 2000

**0029851.3**

3. Full name, address and postcode of the  
or of each applicant  
(underline all surnames)

Sony United Kingdom Limited  
The Heights  
Brooklands  
Weybridge  
KT13 0XW  
United Kingdom

Patents ADP number (if you know it)

652276000

If the applicant is a corporate body, give  
the country/state of its incorporation

UNITED KINGDOM

4. Title of the invention

Transferring Watermarked Material

5. Name of your agent (if you have one)

D. YOUNG & CO

"Address for service" in the United Kingdom  
to which all correspondence should be sent  
(including the postcode)

21 NEW FETTER LANE  
LONDON  
EC4A 1DA

Patents ADP number (if you know it)

59006

6. If you are declaring priority from  
one or more earlier patent  
applications, give the country and  
date of filing of the or each of these  
earlier applications and (if you know  
it) the or each application number

Country

Priority application  
number  
(if you know it)

Date of filing  
(day/month/year)

1st

2nd

3rd

7. If this application is divided or otherwise  
derived from an earlier UK application,  
give the number and filing date of the  
earlier application

Number of earlier  
application

Date of filing  
(day/month/year)

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? (Answer 'Yes' if:

a) any applicant named in part 3 is not an inventor, or  
b) there is an inventor who is not named as an applicant, or  
c) any named applicant is a corporate body.  
See note (d))

YES

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document	Continuation sheets of this form	0
	Description	10
	Claim(s)	11
	Abstract	1
	Drawing(s)	10 10

10. If you are also filing any of the following, state how many against each item	Priority Documents	0
	Translation of Priority Documents	0
	Statement of inventorship and right to grant of a patent (Patents Form 7/77)	0
	Request for preliminary examination and search (Patents Form 9/77)	1
	Request for substantive examination (Patents Form 10/77)	0
	Any other documents (Please specify)	0

11.

I/We request the grant of a Patent on the basis of this application.

Signature

Date

*D Young & Co*

**D YOUNG & CO**  
Agents for the Applicants

7 Dec 2000

12. Name and daytime telephone number of person to contact in the United Kingdom	Richard Pratt	023 80719500
--	---------------	--------------

### Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

### Notes

a) If you need help to fill in this form or you have any questions, please contact the Patent Office on 01645 500505.

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheets should be attached to this form.

d) If you answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

Transferring Watermarked Material

The present invention relates to transferring watermarked material.

Material means one or more of video material, audio material and data material. Video material is generic to still and moving images.

5 It is known to watermark material. Data may be embedded as a watermark in. A watermark may be imperceptible or perceptible in the material. The present invention uses perceptible watermarks.

A watermark may be used for various purposes. It is known to use watermarks for the purpose of protecting the material against, or trace, infringement of the  
10 intellectual property rights of the owner(s) of the material. For example a watermark may identify the owner of the material.

Watermarks may be "robust" in that they are difficult to remove from the material. Robust watermarks are useful to trace the provenance of material which is processed in some way either in an attempt to remove the mark or to effect legitimate  
15 processing such as video editing or compression for storage and/or transmission. The present invention uses robust watermarks. Watermarks may be "fragile" in that they are easily damaged by processing which is useful to detect attempts to remove the mark or process the material.

It is known to offer watermarked images for sale over the internet.  
20 Watermarked images may be downloaded for inspection and for examination for suitability for the users' desired purpose. If the user wishes to purchase an unwatermarked image, the user agrees to conditions of sale, for example an end user License, and pays for the image e.g. by credit card. The user is then able to download the unwatermarked image. See for example <http://www.eyewire.com/help/>.

25 It is desirable to provide a system in which one user (e.g. a seller) is provided with a system for watermarking material and another user (e.g. a buyer) is provided with a secure method and system for removing the watermark, together with a secure system for transferring watermarked material between sellers and buyers.

According to one aspect of the present invention, there is provided a method of  
30 watermarking and transferring watermarked material in a system comprising a transaction server, first and second clients, first apparatus for applying a perceptible

watermark to the material and second apparatus for removing the watermark; the method comprising the steps of:

transferring from the transaction server to the first apparatus (i) data for creating a watermark, the creating data including (a) data defining an invertible  
5 algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier;

using the said first apparatus to apply a material identifier to the material and applying a watermark to the material, using the said creating data;

transferring from the first client to the transaction server the said material  
10 identifier and data for inverting the algorithm including the said at least one key;

transferring the watermarked material to the second apparatus;

deriving the said material identifier from the material;

transferring the identifier from the second client to the transaction server;

subject to predetermined conditions being satisfied, transferring from the  
15 transaction server to the second apparatus watermark removal data associated with the said material identifier, the removal data including at least one key and data defining an algorithm for removing the watermark in conjunction with the key; and

using the second apparatus to remove the watermark using the said removal data.

20 The method allows originators or owners of material to offer it for sale to buyers in a secure manner. The transaction processor allows many sellers to offer material for sale and for many buyers to buy. The transaction processor allows sellers, who have access to a first client and access to a watermarking apparatus to design and apply secure watermarks without needing to know how, in detail, the watermarking is  
25 achieved. Thus apart from knowing how to co-operate with the server, the sellers do not require skills special to watermarking. Likewise buyers who have access to a second client and a watermark removal apparatus do not need such special skills to remove watermarks once they have complied with the said predetermined conditions.

The security key provides security against unauthorised removal of the  
30 watermark. The data for inverting the algorithm including the said at least one key is transferred to the transaction processor, without such data being on or with the material thereby providing further security.

In a preferred embodiment of the invention, the watermark is applied as part of the compression process. That protects the watermark from removal.

5 In a preferred embodiment, the data for applying the algorithm including the said at least one key is stored in data carrier, most preferably a smart card. The smart card is used in the first apparatus for compressing the material and applying the watermark. The smart card is used to securely transfer the data for inverting the algorithm including the said at least one key from the first apparatus to the first client for transfer to the transaction server.

10 The said watermark creating data may be stored on data carrier, most preferably a smart card, in response to a request for the data sent from the first client to the transaction processor. In one embodiment the said data is transferred from the transaction server to the first client and then to the smart card. In another embodiment the smart card, with the creation data stored thereon, may be sent to the operator of the first apparatus by e.g. post.

15 The said watermark removal data may likewise be transferred from the transaction server to the second apparatus in a data carrier, most preferably a smart card.

20 In one embodiment the said data is transferred from the transaction server to the second client and then to the smart card. In another embodiment, a request for the said data is received by the transaction processor and the said data is stored on the smart card and the card is sent to the operator of the second apparatus, e.g. by post.

The watermarked material may be transferred from the first apparatus to the second on a recording medium, for example a disc or tape, by for example post. Alternatively, the watermarked material may be transferred via the an electronic communications network, possibly in compressed format.

25

Other aspects of the invention are specified in the claims to which attention is invited.



For a better understanding of the present invention, reference will now be made by way of example to the accompanying drawings in which:

Figure 1 is a schematic diagram of a material transfer system in accordance with an embodiment of the invention;

5        Figure 2 is a schematic diagram illustrating seller registration;

Figure 3 is a schematic diagram of an example of a smart card;

Figure 4 is a schematic diagram of another example of a smart card;

Figure 5 is schematic diagram illustrating material acquisition;

10       Figure 6 is a schematic diagram illustrating the application of the invention to legacy material;

Figure 7 is a schematic diagram of a tape on which a material identifier and watermarked material is recorded;

Figures 8 and 9 illustrate transaction server functions; and

Figure 10 is schematic diagram illustrating material purchase.

15       Overview, Figure 1.

Referring to Figure 1, a system in accordance with the invention comprises a transaction server, a seller client 2, a buyer client 3 and a communications network 4 linking the clients to the server.

20       The owner of material, i.e. the seller, controls the seller client 2. A buyer controls the buyer client 3. A third party owns and controls the transaction processor 1. The system allows material to be acquired, securely watermarked, and transferred to the buyer for the buyer to preview (9) the watermarked material. If the buyer then wants to buy the material, the buyer obtains from the transaction server 1 the data needed to remove the watermark. In this example, the seller and buyer both register  
25       (10) with the transaction server. Registration, content preview, and watermark removal are described in more detail hereinbelow. The data for removal of the watermark is sent to the buyer only when the buyer has paid for the material. The payment is monitored by the transaction server 1 which communicates with a financial institution 8. Payment is made via the server 1 and/or via the institution 8.

30       Associated with the seller client 2 is a first apparatus 5 for compressing video material and for applying a watermark to the material as part of the compression process. An example of such apparatus and process are disclosed in copending

application 00 , attorney file P/10145, I-00-147 the content of which is incorporated herein by virtue of this reference to it. Figure 1 denotes such apparatus at 5 by "legacy" and "acquisition" which will be described in more detail below in the sections "legacy" and "acquisition". Associated with the buyer client 3 is a second apparatus 6 for removing the watermark. An example of such apparatus and process are disclosed in copending application 00 , attorney file P/10145, I-00-147 the content of which is incorporated herein by virtue of this reference to it. Figure 1 denotes such apparatus at 6 by "content purchase" which will be described in more detail below in the section "content purchase".

10 In this example the material is video material and is recorded on a tape 7 which will be described in more detail with respect to Figure 7. The material is acquired and watermarked by the first apparatus 5. In addition a material identifier is applied to the material. Then the material is transferred on the tape to the second apparatus 6. The transfer is for example by post.

15 An identifier is applied to the material. An example of an identifier is a Unique Material Identifier or UMID. UMIDs are described in more detail in SMPTE Journal March 2000.

#### Seller Registration, Figure 2.

The seller client 2 is used to send to the transaction server 1 a) passwords, b) bank account details of the seller and c) any other information. The transaction server may then send data carrier, in this example a smart card SC, to the seller. The seller inserts the smart card into the client 2 and communicates with the server 1. The seller designs the form of the watermark to be applied to the material using the server. The form of the watermark is defined by a bit map, also referred to herein as the template. The seller also obtains from the server an algorithm for creating the watermark including one or more security key generators for applying the watermark and a UMID generator. The template, algorithm, key generators and UMID generator are downloaded onto the smart card for transfer to the seller.

#### Smart Card, Figures 3 and 4.

30 Smart cards are well known. A smart card may have a processor and memory as shown in Figure 3, or may have memory but no processor as shown in Figure 4.

In the example of Figure 3, the card SC has a processor SC1, a template store SC2, a key generator SC3, a UMID generator SC4 and a store SC5. The template store SC2 stores the template defining the form of the watermark. The processor is programmed to implement the algorithm. The processor SC1 receives the image to be watermarked and uses the keys generated by the generator SC3 and the template to apply the watermark. Keys generated by the generator SC3 are stored in the store SC5. Each piece of material is assigned a UMID. Each UMID is also stored in store SC5 in association with the keys generated for that piece of material.

In the example of Figure 4, the smart card contains only memories SC5', SC2' and SC6. SC5' is a UMID and key store, SC2' is a template store and SC6 stores algorithm configuration data. The card of Figure 4 operates in conjunction with an external processor to apply a watermark to material. UMIDs and keys generated in that process are stored in the store SC5'.

#### Acquisition, Figure 5.

Referring to Figure 5, new material is acquired using a camera 50. A blank tape 51 is inserted into the camera 50. Also a smart card SC is inserted into an interface in the camera. This example assumes that the card is as shown in Figure 3 and has a processor SC1. The camera 50 produces image data (which may be DCT coefficients) which are applied to the processor in the card SC. The card applies the watermark defined by the stored template and the algorithm and keys. The card also generates one or more UMIDs to identify the material recorded on the tape. The UMIDs and keys so generated are stored in store SC5 on the card. The UMIDs are also recorded on the tape (see Figure 7 below).

The card SC is removed from the camera 50 and inserted into the seller client 2. The data stored on the card is transferred to the server 1 via the network 4. In addition the seller may record on the smart card and transfer to the server 1 data such as price, and conditions of sale. In addition metadata relating to the material may be transferred. The UMIDs provide references which uniquely identify the material and the data associated with it which are transferred to the server 1.

#### Legacy Material, Figure 6.

Legacy material is "old " material which did not have a watermark applied according to the present invention when first acquired. Such legacy material

may be stored on tape or in other storage 61, for example an A/V server. In the system of Figure 6, a VTR 62 has an interface for receiving a smart card SC and also a port for receiving material from the A/V server 61. Also an unwatermarked tape 60 containing legacy material may be inserted into the VTR 62. The VTR operating with the smart card SC applies a watermark and UMID to the legacy material and the generated keys and UMIDs are stored in the card SC as described above. The card SC is inserted into the seller client for transfer, via network 4, of its data, plus any other data such a price and conditions of sale, as described above in relation to acquisition to the transaction server 1.

Figure 6 shows the VTR 62 and seller client as part of a Local Area Network having at least one workstation 2'. That work station has an interface for receiving a smart card. Legacy material from the A/V store 61 may be routed to the workstation which co-operates with the smart card to apply a watermark to the material which is then stored in the store 61. The UMIDs and keys generated during the process of watermarking are stored on the card SC. The PC may retrieve the data stored on the card and send it to the server 1.

Watermarked material may be stored on the A/V server 61 and also on tape 60.

#### Tape. Figure 7.

Referring to Figure 7, an example of a tape 51 or 60 is shown.

Watermarked Video is stored in conventional manner in helical tracks 70. The tape has a conventional control track 72 in which time codes are recorded. The UMIDs are recorded in the user bits of the time codes. That is described in more detail in copending application 9926321.3,( also EP 00309067.7), attorney file P/7211, I-99-41.

#### Transaction Server. Figure 8

The transaction server 1 provides secure communications with the seller and buyer clients. It also controls financial transactions by holding buyer and seller accounts. As described above, the seller registers passwords, bank account details with the server 1. In addition, the server provides algorithm specifications and registration, and provides a system for designing templates. It establishes rules for UMIDs. It also provides for the secure uploading and storage of keys and UMIDs generated during watermarking. Metadata may also be uploaded and stored in the

server 1 . The UMIDs provide references for associating the stored data with the material to which that data relates.

The transaction server may store multiple different algorithms for creating and removing watermarks, in addition to the currently preferred and inventive algorithm  
5 which is described in copending application I-00- 147, P/10145, Application 00

The transaction processor also monitors buyer interest and sales and controls the release of data for removing watermarks; such data is not released unless the server has confirmation that the buyer satisfies the conditions of sale including paying for the material.

10 The transaction server 1 also controls the distribution of smart cards.

---

Transaction Server, Figure 9

The transaction server also provides for the registration of data relating to the buyers. For example, the buyer provides details of bank accounts, passwords and any other data relevant to a transaction.

15 The registration of the buyer allows access to:

- a) business rules, prices and conditions of sale to enable the buyer to purchase the material; and
- b) data, such as metadata, relating to material received by the buyer and which the buyer has bought or which he might buy.

20 Once the buyer has satisfied the conditions of sale, the transaction server provides secure delivery of decryption keys templates and algorithms for removing watermarks. That may be done by securely downloading data to smart cards as described above and sending the smart cards to the buyers.

25

Content Purchase, Figure 10.

Referring to Figure 10, a buyer receives watermarked material and previews it on a VTR 101. If the buyer is interested in the material, he accesses the UMID recorded on the tape and registers his interest in the material with the transaction  
30 server using the UMID as a reference via the buyer client 3 and the network 4. The transaction server provides to the buyer the conditions of sale and price. If the buyer

then agrees to buy, the buyer provides payment and requests the data needed to remove the watermark.

Payment may be by automatic transfer from his bank account previously registered with the server 1 or by other means which the server can monitor. Once the server 1 has confirmation of payment, the server 1 provides the watermark removal data. That data is downloaded via the buyer client 3 to a smart card SC as described above for example. The smart card is inserted into an interface in the VTR 101 which then co-operates with the card to remove the watermark. In this example the card is assumed to be a card as shown in Figure 3.

Instead of receiving watermarked material on tape or other recording medium, the watermarked material may be accessed from an A/V store 102.

The embodiments of the invention have been described with reference to video material. However the invention is also applicable to audio/visual material, to audio material and to other data material.

Whilst the foregoing refers to transferring material on tape via a physical communications network such as the Post, the material could be transferred via an electronic network, most preferably a broad-band network.

The network 4 may be the web as shown in the figures. It could be any other communication network.

Transfer of data between the server and the clients is preferably carried out in a secure manner using security techniques known in the art of secure communications.

#### Modifications.

The examples of the invention described above use a smart card for transferring data. The data may be transferred on other data carriers. Smart cards are advantageous because they provide security for the data. Data may be carried on other carriers preferably in encrypted form for security. Most preferably, the data carrier is hand insertable into an interface.

The transaction server contains metadata relating to the watermarked material. That metadata preferably includes samples and/or extracts of the watermarked material to allow potential buyers to browse the material available. For example for video, low resolution frames and/or video sequences may be browsed. The metadata also may include text describing the material which may be searched and which is also

preferably linked to the samples of the material. Thus, for example a video sequence of a well known person may be accessed by searching for his or her name. Once found the buyer can request that the tape of the watermarked video be transferred to him.

- 5           The examples of the invention described above refer to video material. The invention may be applied to moving and still images. The invention may be applied to audio material or to data material. Preferably it is applicable to audio/visual material.
-

## CLAIMS

1. A method of watermarking and transferring watermarked material in a system comprising a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark; the method comprising the steps of:
- 5       transferring from the transaction server to the first apparatus (i) data for creating a watermark, the creating data including (a) data defining an invertible algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier;
- 10       using the said first apparatus to apply a material identifier to the material and applying a watermark to the material, using the said creating data;
- transferring from the first client to the transaction server the said material identifier and data for inverting the algorithm including the said at least one key;
- transferring the watermarked material to the second apparatus;
- 15       deriving the said material identifier from the material;
- transferring the identifier from the second client to the transaction server;
- subject to predetermined conditions being satisfied, transferring from the transaction server to the second apparatus watermark removal data associated with the said material identifier, the removal data including at least one key and data defining
- 20       an algorithm for removing the watermark in conjunction with the key; and
- using the second apparatus to remove the watermark using the said removal data.
2. A method according to claim 1, wherein the first apparatus compresses the
- 25       material and applies the watermark as part of the compression process.
3. A method according to claim 1, 2 or 3, wherein the said data defining the invertible algorithm comprises algorithm configuration data.
- 30       4. A method according to claim 1, 2 or 3, wherein the said data defining the invertible algorithm comprises the algorithm.



5. A method according to claim 1, 2, 3, 4 or 5, wherein data for creating the material identifier is stored in a data carrier for transfer to the first apparatus.
6. A method according to claim 1, 2, 3, 4 or 5, wherein the said data for creating a watermark is stored in a data carrier for transfer to the first apparatus.
7. A method according to claim 6, wherein a material identifier and at least one key are generated during the application of the watermark to the material, and comprising the step of storing the generated identifier and key on a data carrier for transfer to the first client for transfer to the transaction server.
- 
8. A method according to any preceding claim, comprising the step of storing in the transaction server metadata relating the said watermarked material, the metadata being referenced by the said identifier.
9. A method according to any one of claims 1 to 8, wherein the said removal data is stored in a data carrier for transfer to the second apparatus.
10. A method according to any preceding claim, comprising storing on the transaction server conditions of sale of unwatermarked material.
11. A method according to claim 10, comprising the step of transferring the said conditions of sale from the first client to the transaction server.
12. A method according to claim 10 or 11, wherein the transaction server transfers the said removal data subject to the condition that a buyer has fulfilled the conditions of sale.
13. A method according to any preceding claim, comprising the step of storing the watermarked material in a recording medium and transferring the watermarked material to the second apparatus on the recording medium.

14. A data carrier in which is stored (i) data for creating a watermark, the creating data including (a) data defining an invertible algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier.

5

15. A data carrier according to claim 14, wherein the carrier is a smart card comprises a processor and memory and the processor is programmed to implement the said algorithm.

10 16. A data carrier according to claim 14, wherein the carrier is a smart card comprises memory storing algorithm configuration data defining the invertible algorithm.

---

15 17. A data carrier in which is stored watermark removal data including at least one key and data defining an algorithm for removing a watermark in conjunction with the key.

18. A data carrier according to claim 17, wherein the carrier is a smart card comprises a processor and memory and the processor is programmed to implement the  
20 said algorithm.

19. A data carrier according to claim 17, wherein the carrier is a smart card comprises memory storing algorithm configuration data defining the invertible  
25 algorithm.

25

20 A system comprising a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark, the said first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing  
30 the watermark being linked by one or more communications networks; the system being arranged to implement the method of any one of claims 1 to 13.

21. A method or system according to any preceding claim wherein the said material is video material.
22. A method or system according to any one of claims 1 to 20 wherein the said material is audio/visual material.
23. A method or system according to any one of claims 1 to 20 wherein the said material is audio material.
24. A method or system according to any one of claims 1 to 20 wherein the said material is data material.
- 
25. A data processing apparatus comprising  
an information material processing apparatus operable to receive signals  
representative of information material, and to adapt said signals to the effect of  
introducing a reversible modification to said information material in accordance with a  
modification key, said modification being arranged to provide a disturbing effect on  
the information material to a human recipient,  
a data generation processor operable to generate data identifying said  
information material,  
a recording apparatus operable to record said adapted signals and said  
identifying data on a recording/reproducing medium, and  
a data processor operable to receive said identifying data and said modification  
key and to store said identifying data and data representative of said modification key  
data on a data carrier.
26. An apparatus as claimed in Claim 25, wherein said recording/reproducing medium is a linear recording medium including capacity for ancillary data, and said identifying data is recorded in said capacity for recording time codes.
27. An apparatus as claimed in Claim 25 or 26, wherein said data carrier is a hand insertable carrier.

28. An apparatus as claimed in Claim 27, wherein said data carrier is a smart card or the like.

5 29. An apparatus as claimed in any of Claims 25 to 28, wherein said identifying data is a Unique Material Identifier or the like.

30. An apparatus as claimed in any one of Claims 25 to 29, said apparatus comprising

10 an information material server arranged to store signals representative of information material, and to retrieve selected signals representative of selected information material items, said information material processing apparatus being operable to adapt said selected signals, said data generation processor being operable to generate said data identifying said selected information material signals.

15

31. A camera comprising the apparatus according to any of Claims 25 to 30.

32. An apparatus for receiving a data carrier having data stored by the apparatus according to any of Claims 25 to 31, said apparatus comprising

20 a data reading processor operable to receive said data carrier via hand insertion by a user and to read the modification key and the identifying data, and  
a communications processor operable to communicate said modification key and said identifying data to a data base processor.

25 33. An apparatus as claimed in Claim 32, wherein said communications processor is operable to communicate said modification key and said identifying data to said data base processor via a communications network.

30 34. An apparatus as claimed in Claim 33, wherein said communications network is the world wide web.

35. An apparatus as claimed in any of Claims 32 to 34, wherein said communications processor is operable to receive data representative of sales conditions and price information and to communicate said sales conditions and said price information with said modification key data and said identifying data to said data  
5 base processor.

36. A signal bearing the modification key and the identifying data generated by the apparatus according to any of Claims 32 to 35.

10 37. A signal ensemble comprising the adapted signals representing audio and/or video signals adapted by the apparatus as claimed in any of Claims 25 to 31, and the signal bearing the modification key and the identifying data generated by the apparatus according to any of Claims 32 to 36.

15 38. A method comprising the steps of:  
applying, using a watermarking apparatus, a removable perceptible watermark to material, the watermark being removable using removal data created during application of the watermark and applying identifying data to the material to identify the watermarked material;  
20 registering with a transaction server conditions for the removal of the watermark and identifying data identifying the watermarked material;  
transferring the watermarked material to a watermark removal apparatus; and  
identifying to the server the transferred material, and transferring the  
25 removal data to the removal apparatus to allow removal of the watermark if the transaction server indicates that predetermined conditions for removal are satisfied.

39. A method according to claim 38, wherein the said conditions are conditions of  
30 sale of the material.

40. A method according to claim 39 wherein the conditions of sale include paying for the material.

5 41. A method according to claim 38 or 39 or 40, comprising the step of using a first client linked to the transaction server by a communications network to register the said conditions.

42. A method according to claim 41, comprising the step of using a second client linked to the transaction server by a communications network to comply with the said  
10 conditions.

---

43. A method according to any one of claims 38 to 42, comprising the steps of loading the removal data onto a data carrier and transferring the carrier to the removal apparatus when the said conditions are satisfied.  
15

44. A method according to claim 43, wherein the removal data is downloaded onto the data carrier from the transaction server via the communications network.

20 45. A method according to claim 44, wherein the data carrier is a smart card.

46. A system comprising a watermarking apparatus, a transaction server and a watermark removal apparatus arranged to carry out the method of any one of claims 38 to 45.

25 47. A server arranged to:  
a) receive and store data identifying watermarked material, data enabling removal of the watermarks from material and data setting predetermined conditions for the removal of watermarks; and  
b) receive identifying data identifying watermarked material form  
30 which a watermark is to be removed;  
c) monitor whether the predetermined conditions are satisfied; and

d) if the conditions are satisfied, providing the removal data for transfer to apparatus for removal of the watermark.

48. A server according to claim 47, wherein the said predetermined  
5 conditions are conditions of sale of the material.

49. A server according to claim 48, arranged to receive and store financial data relating to the sellers of the watermarked material.

10 50. A server according to claim 48 or 49, arranged to receive and store financial data relating to buyers of the watermarked material.

---

51. A server according to claim 48, 49 or 50, wherein the said conditions of sale include paying for the material.

15 52. A server according to claim 51, wherein the server is arranged to monitor transfer of money from the buyer to the seller.

53. A server according to claim 52, which is linked by a communications  
20 network with a financial institution to monitor the said transfer of money.

54. A server according to any one of claims 47 to 53 , wherein the removal data includes a template and a security key.

25 55. A server arranged to:  
interact with a client so as to enable a user of the client to design a template of a watermark; and

output a watermarking algorithm, or data for configuring such an algorithm, and data for generating security keys for implementing the algorithm.

56. A server according to claim 55, arranged to output the said algorithm or configuring data and the key generating data to a data carrier for transfer to the said user.

5 57. A server according to claim 56, wherein the data carrier is a smart card.

58. A data processing apparatus arranged to :

a) transfer, to a server via a communications network, data identifying watermarked material and a request for removal data enabling the removal of the  
10 watermark from the identified material; and

b) receive the removal data.

59. Apparatus according to claim 58, comprising an interface for receiving a data carrier, the apparatus being arranged to transfer the removal data to the carrier  
15 when the carrier is received by the interface.

60. A system according to claim 58, further comprising a store storing watermarked material, the apparatus being arranged to receive the said material from the store; and to remove the watermark using the said removal data.  
20

61 A system according to claim 60, arranged to store the material from which the watermark has been removed in the said store.

62 Apparatus for removing a watermark from watermarked material,  
25 comprising:

a first port for receiving the said watermarked material; and  
a second port for receiving watermark removal data.

63. Apparatus according to claim 62, wherein the first port is arranged to  
30 receive a first data carrier on which the said material is recorded; and  
the second port is arranged to receive a second data carrier on which the said removal data is recorded.



64. Apparatus according to claim 63 wherein the second port is arranged to receive a smart card.

5           65. Apparatus according to claim 63 or 63 wherein the first port is arranged to receive a tape record.

66. A watermark removal system comprising apparatus any one of claims 62 to 65 and an apparatus or system according to any one of claims 58 to 61.

10

---

67. A signal comprising watermark removal data including a key and an algorithm or data for configuring an algorithm.

68. A signal according to claim 67, further including a watermark template.

15

69. A signal ensemble comprising a signal according to claim 66, 67 or 68 and a separate signal including the watermarked material.

70. A method comprising the steps of:

20           receiving, via a first channel, material which is watermarked with a watermark which is reversible; and

            receiving, via a second channel, removal data which enables the removal of the watermark.

25           71. A method according to claim 70, wherein the first and second channels follow different paths.

72. A method according to claim 70 or 71, further comprising the step of removing the watermark using the removal data.

30

73. A transaction server substantially as herein before described with reference to Figures 1 to 10.

74. A seller client substantially as herein before described with reference to Figure 2, 6 and/or 8.

75. A buyer client substantially as herein before described with reference to Figure 9 and/or 10.

76. A method of watermarking and transferring watermarked material substantially as hereinbefore described with reference to the accompanying drawings.

---

77. A system of watermarking and transferring watermarked material substantially as hereinbefore described with reference to the accompanying drawings.

78. A computer program product arranged to implement the method of any one of claims 1 to 13 and 21 to 25 when run on a system comprising a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark.

AbstractTransferring watermarked material.

5           A system for watermarking and transferring watermarked material comprises a transaction server, first and second clients, first apparatus for applying a perceptible watermark to the material and second apparatus for removing the watermark. The server, clients and first and second apparatus are linked by one or more communications networks. The system is arranged to implement the steps of:

10           transferring from the transaction server to the first apparatus (i) data for creating a watermark, the creating data including (a) data defining an invertible algorithm and (b) data for creating at least one security key associated with the algorithm and (ii) data for creating a material identifier;

            using the said first apparatus to apply a material identifier to the material and

15           applying a watermark to the material, using the said creating data;

            transferring from the first client to the transaction server the said material identifier and data for inverting the algorithm including the said at least one key;

            transferring the watermarked material to the second apparatus;

            deriving the said material identifier from the material;

20           transferring the identifier from the second client to the transaction server;

            subject to predetermined conditions being satisfied, transferring from the transaction server to the second apparatus watermark removal data associated with the said material identifier, the removal data including at least one key and data defining an algorithm for removing the watermark in conjunction with the key; and

25           using the second apparatus to remove the watermark using the said removal data.

[No Figure].

# System Overview

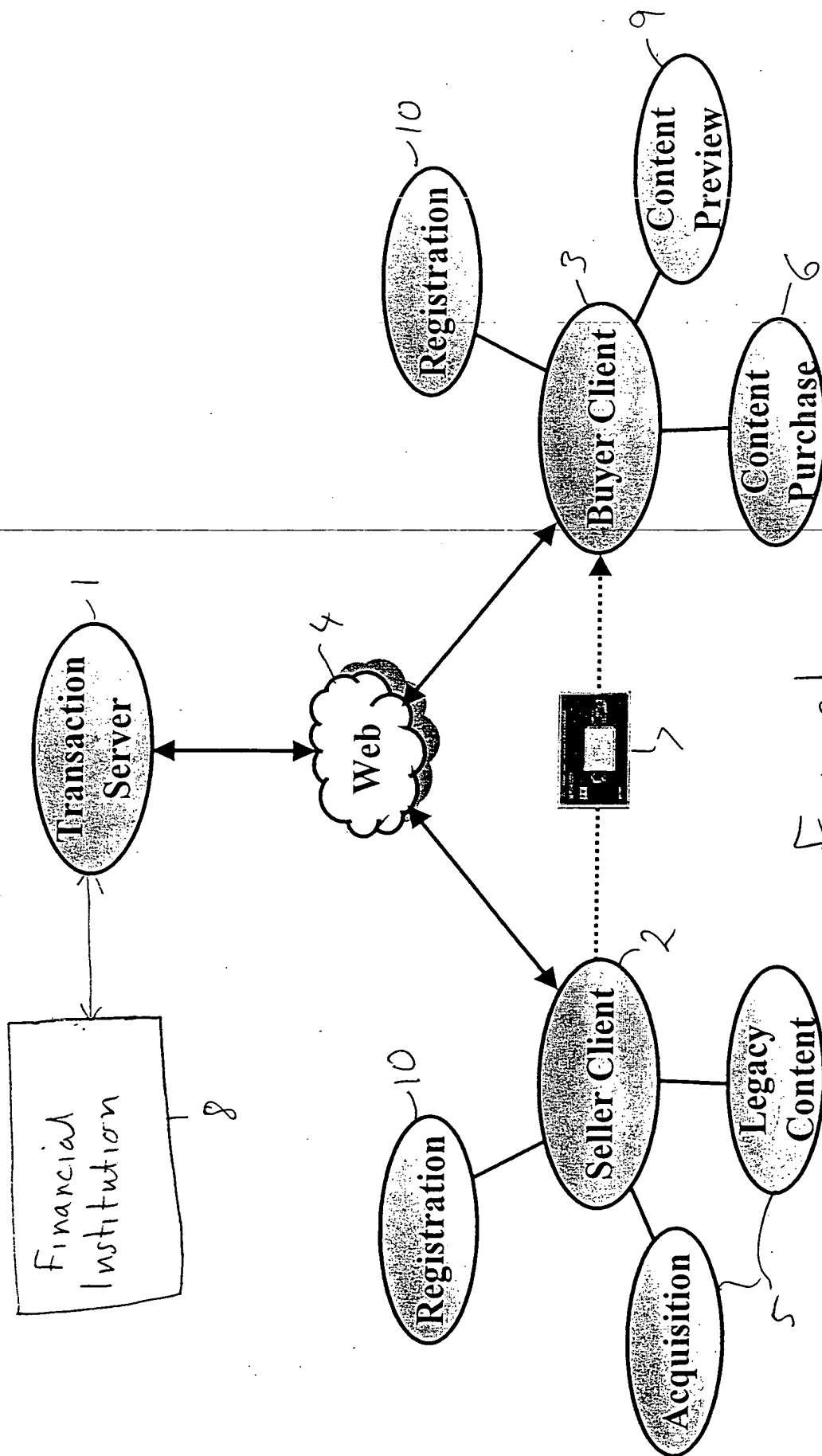
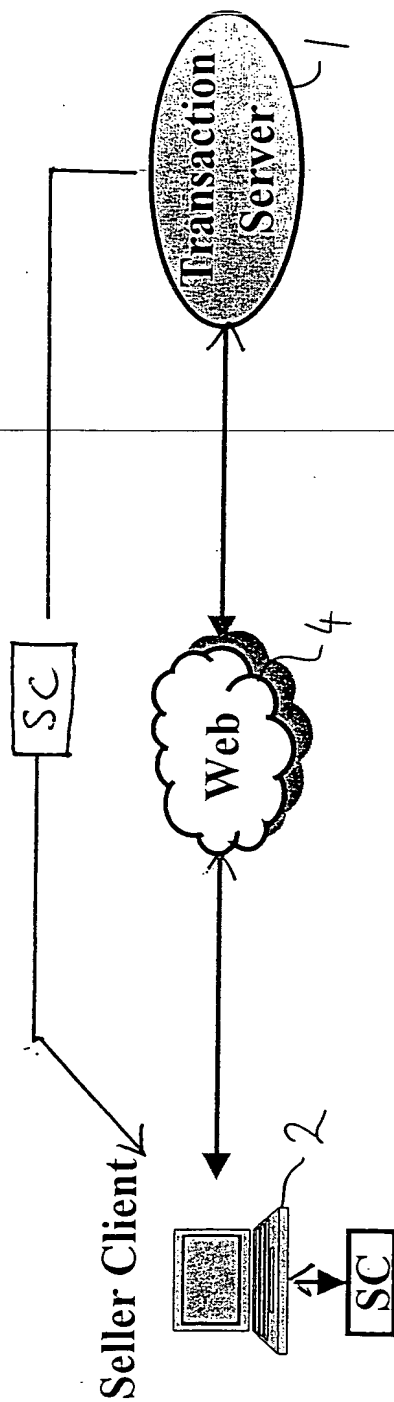


Figure 1

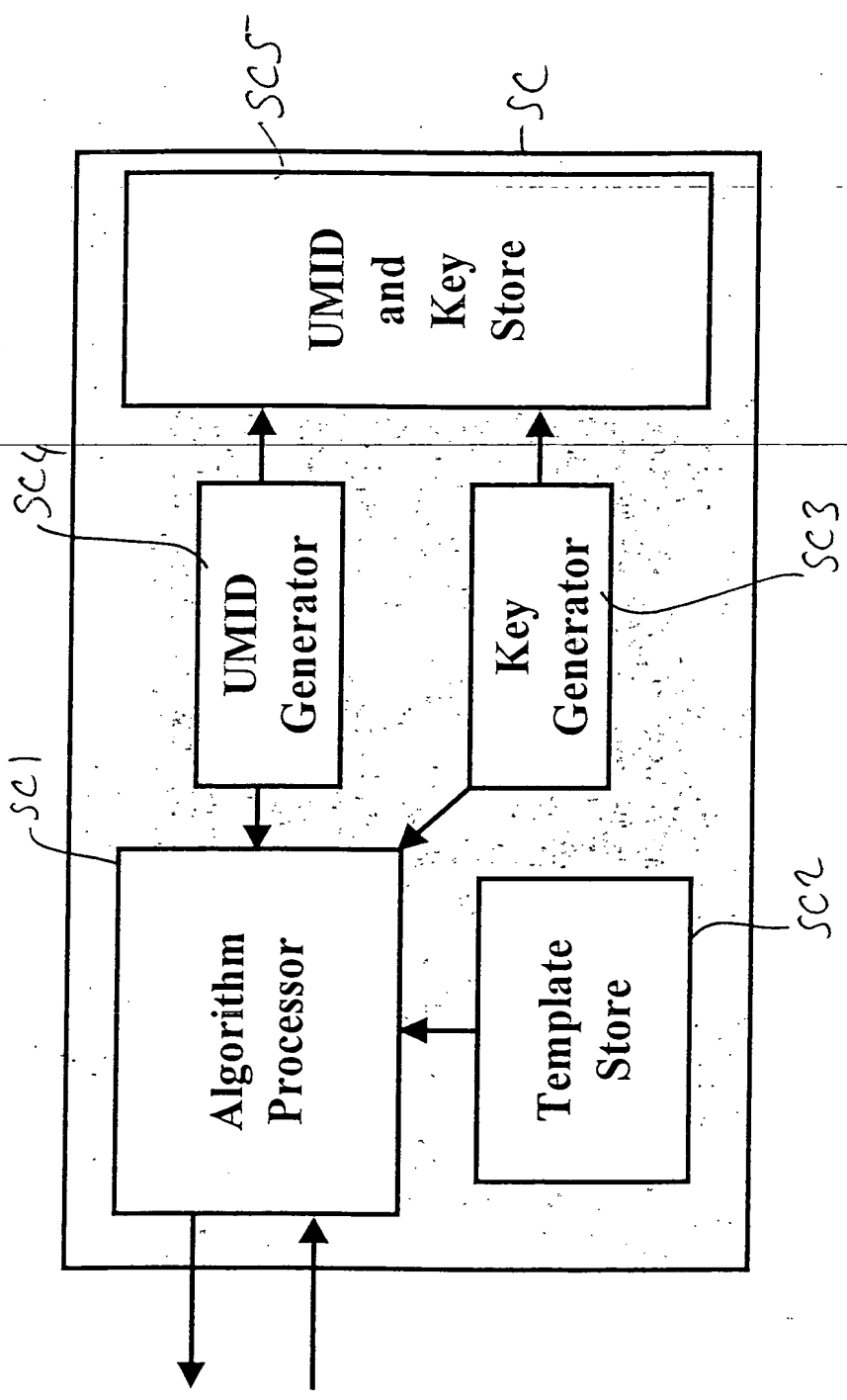
# Seller Registration



- Seller registers with transaction-server, setting passwords, bank account details etc.
- Transaction-server sends smart-card to seller
- Seller designs template and chooses algorithm using the transaction-server web-site
- Seller's smart-card is configured

Figure 2

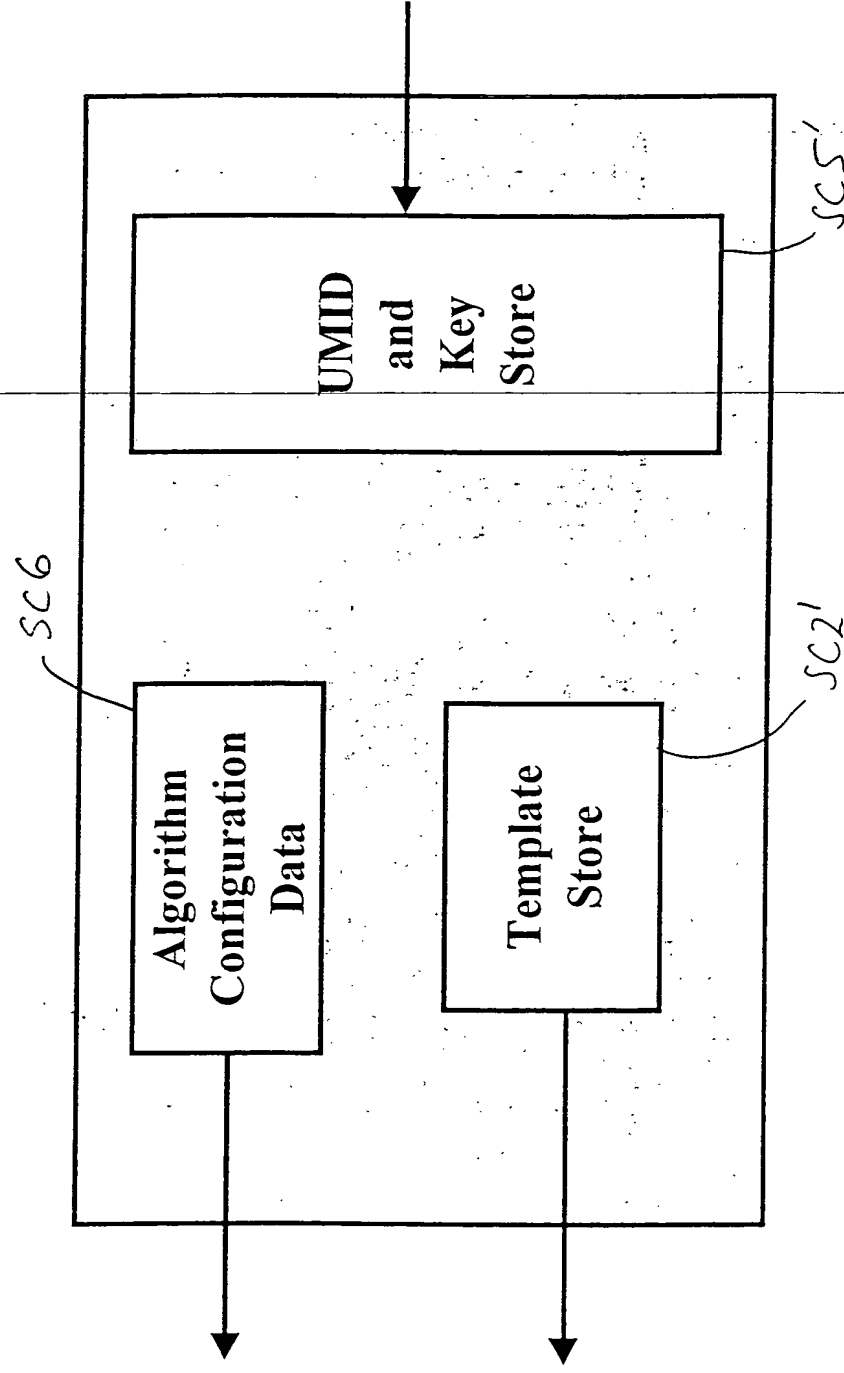
# Smart-Card ( processor)



- All algorithmic processing, key generation and UMID generation is performed on the smart-card

Figure 3

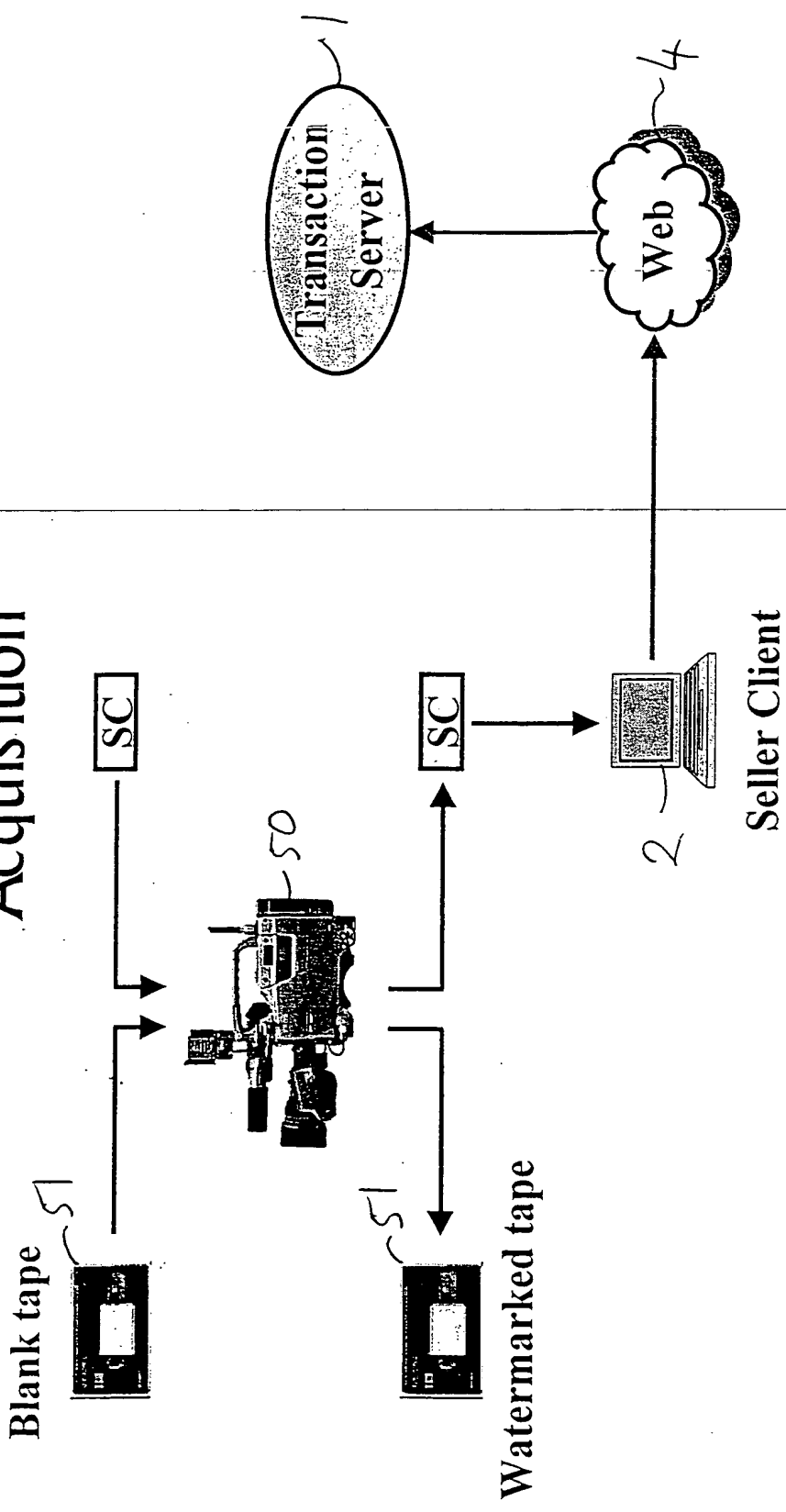
# Smart-Card (memory)



- Smart-card initialised with algorithm configuration data and template
- Generated UMIDs and keys are loaded onto the smart-card

Figure 4

# Acquisition

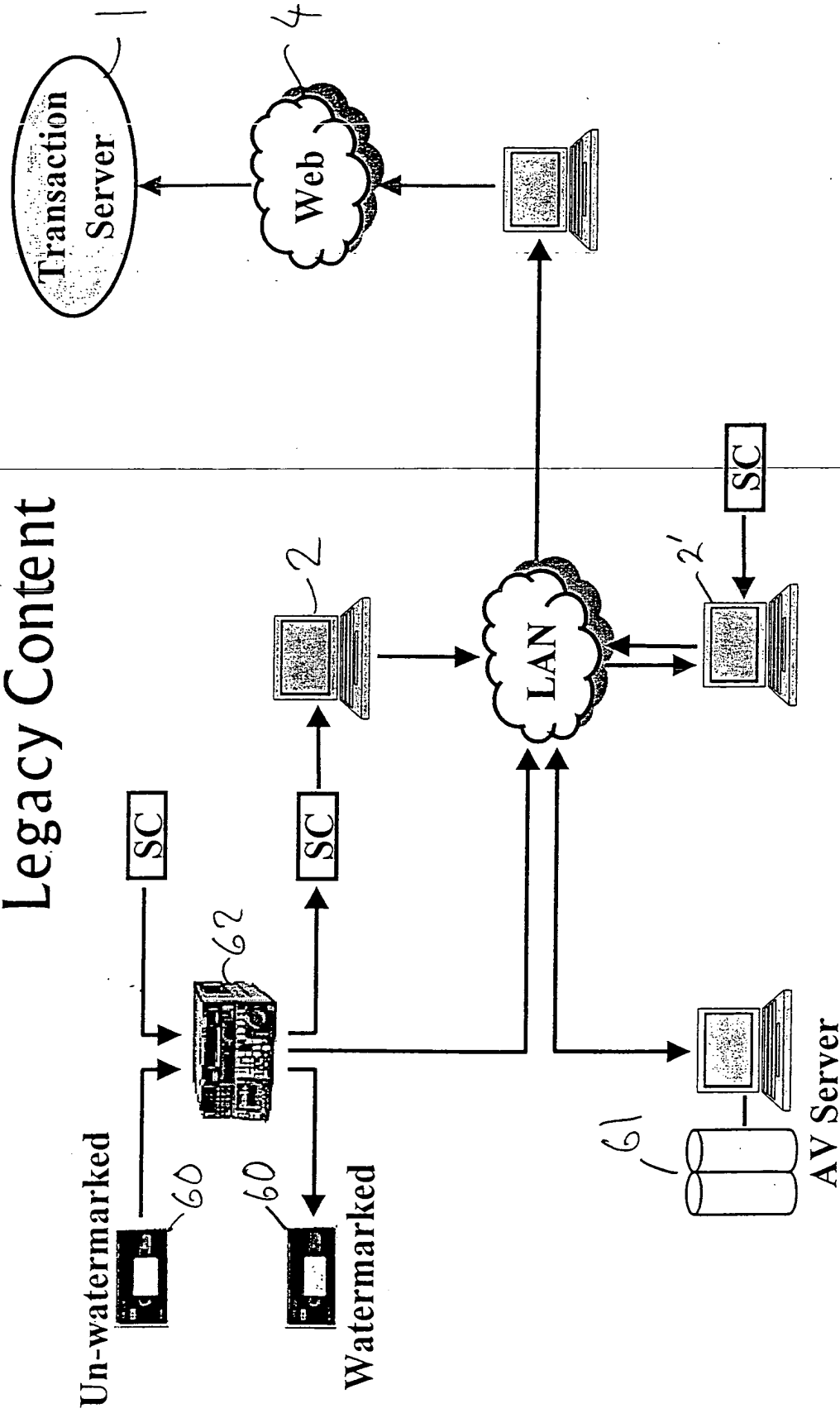


- Upload transaction-server with UMIDs, keys, metadata, price information, conditions-of-sale, etc.

Figure 5



# Legacy Content



- Upload transaction-server with UMIDs, keys, metadata, price information, conditions of sale, etc.

Figure 6

# Watermarked Tape

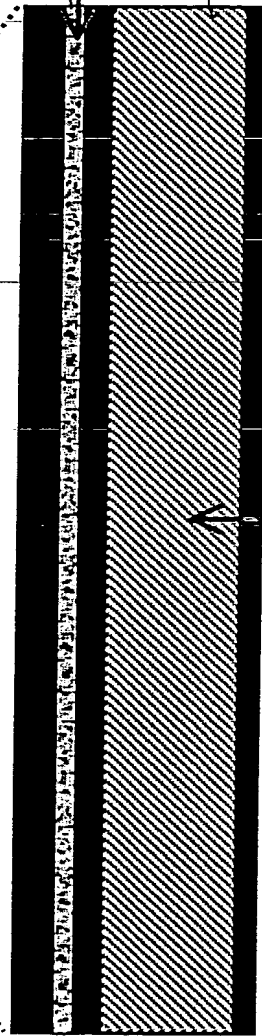
60, 51



72

UMIDs  
in user-bits

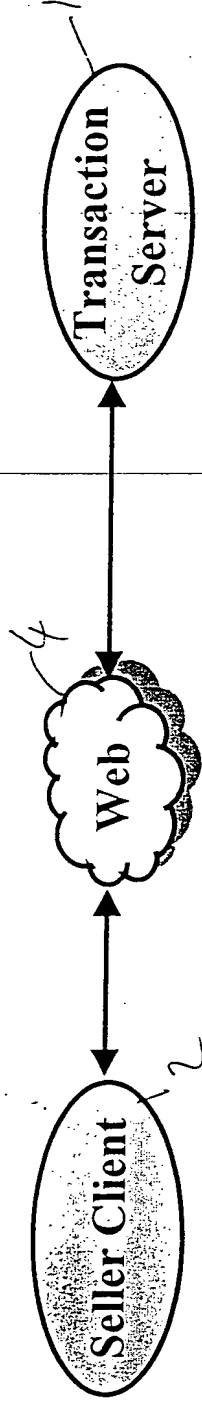
70



Compressed and visibly-watermarked  
video

Figure 7

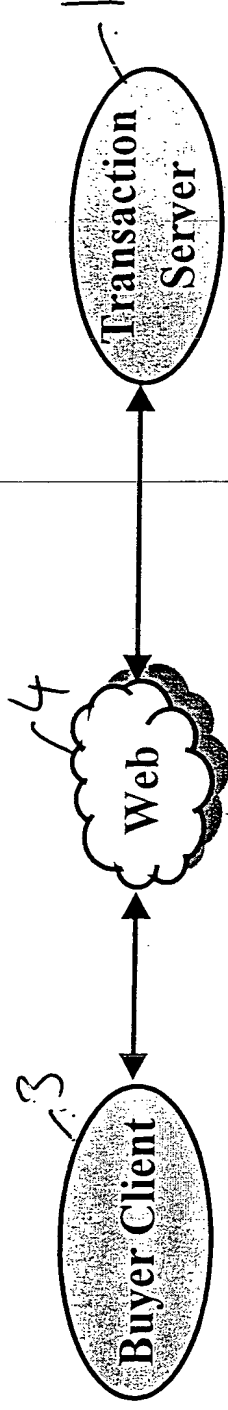
## Transaction Server Functions (Seller)



- Seller registration (approval, passwords, bank account details etc.)
- Visible watermark template design, validation and registration
- Algorithm specification and registration
- Establish business rules for UMIDs
- Publish metadata (clip-length, time & date etc.)
- View / monitor buyer interest and sales
- Secure upload of keys and UMIDs for watermarked content (SSL)

Figure 8

## Transaction Server Functions (Buyer)



- Buyer registration (approval, passwords, bank account details etc.)
- Access to metadata
- Register interest in UMIDs
- Access business rules and pricing – enable purchase
- Secure delivery of decryption-keys, templates and algorithms (SSL)

Figure 9

# Content Purchase

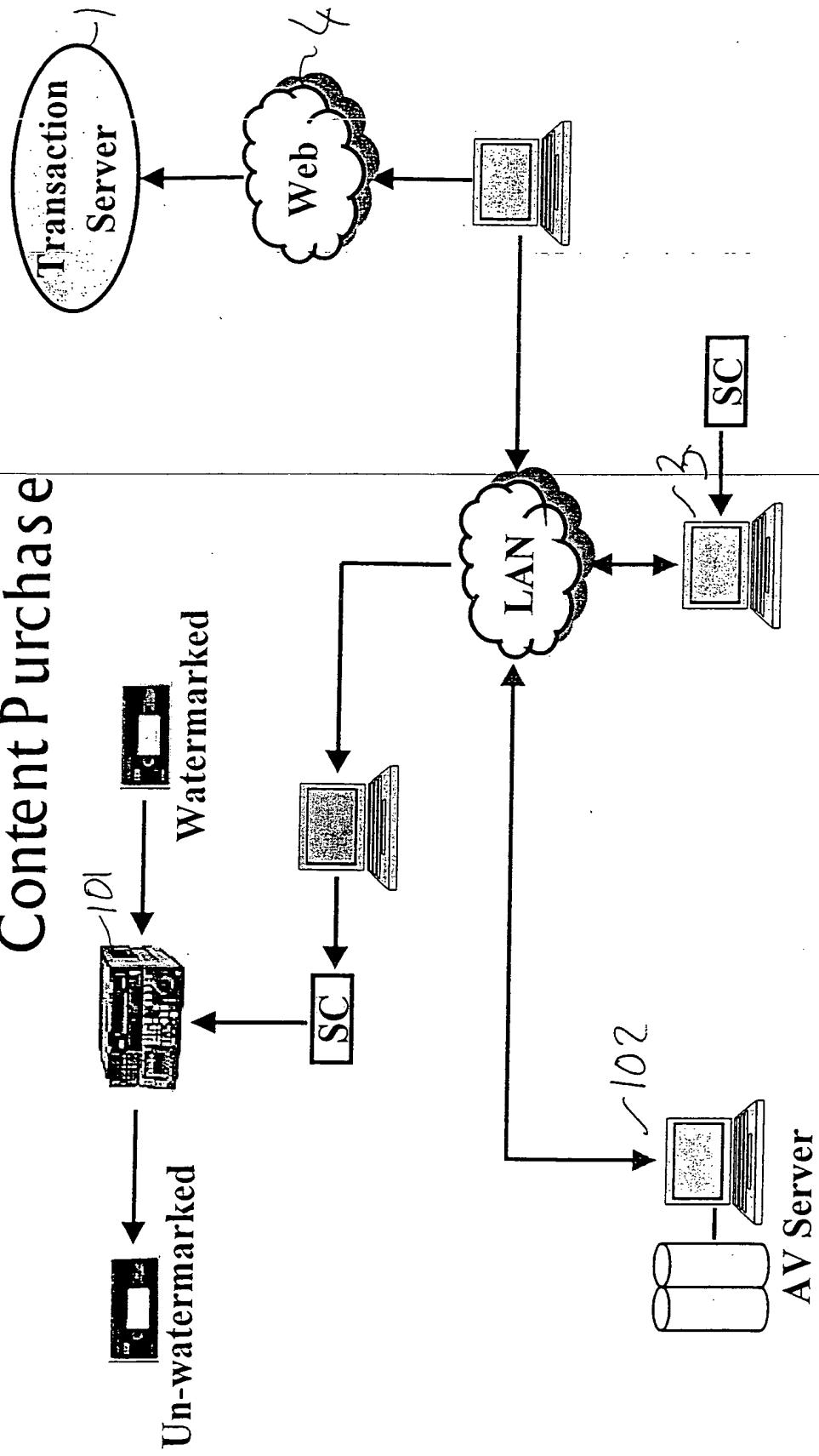


Figure 10